(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09305661 A**

(43) Date of publication of application: **28 . 11 . 97**

(51) Int. Cl **G06F 17/60**
G06F 15/00
G09C 1/00
G09C 1/00
H04L 9/32

(21) Application number: **08116012**

(22) Date of filing: **10 . 05 . 96**

(71) Applicant: **HITACHI LTD**

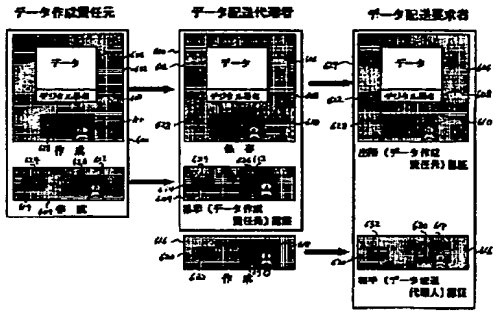
(72) Inventor: **KAWAZURE YOSHIAKI**
CHIBA HIROYUKI

(54) SOURCE AUTHENTICATING METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a souce authenticating method for making the generation responsible source of transmission data clear.

SOLUTION: A means for mutually authenticating two parties actually executing communication is buried in an electronic envelope part (604 and 616) and a means for authenticating a data generation responsible person by a data delivery requesting person is buried in a ciphering data part (602) so that a data dilivery agent authenticates the data generation resonsible source by the electronic envelope 604 part. The electronic envelope is re-generated so as to permit the data delivery requesting person to authenticate the data delivery agent (616) and delivered to the data delivery requesting person so that the data delivery agent is authenticated and the data source is authenticated by a cipher or data 622 part.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－305661

(43)公開日　平成９年(1997)11月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	17/60			Ｇ０６Ｆ	15/21	Ｚ
	15/00	３３０			15/00	３３０Ａ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ａ
			7259－5Ｊ			６４０Ｂ
		６６０	7259－5Ｊ			６６０Ｅ

審査請求　未請求　請求項の数１　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平8－116012

(22)出願日　平成８年(1996)５月10日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　川連　嘉晃
神奈川県横浜市都筑区加賀原二丁目２番株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者　千葉　寛之
神奈川県横浜市都筑区加賀原二丁目２番株式会社日立製作所ビジネスシステム開発センタ内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　出所認証方法

(57)【要約】
【課題】本発明は送付データの作成責任元を明確化する出所認証方法を提供することにある。
【解決手段】実際に通信する２者間がお互いを認証する手段を電子封筒部分（６０４、６１６）に、データ配送要求者がデータ作成責任者を認証する手段を暗号化データ部分に埋め込む（６０２）ことにより、データ配送代理人は、電子封筒６０４部分でデータ作成責任元を認証することができ、また、電子封筒を、データ配送要求者が、データ配送代理人を認証できるように再作成して（６１６）、データ配送要求者に配送することにより、データ配送代理人を認証することができ、また、暗号かデータ６２２部分により、データの出所認証をする事ができる。

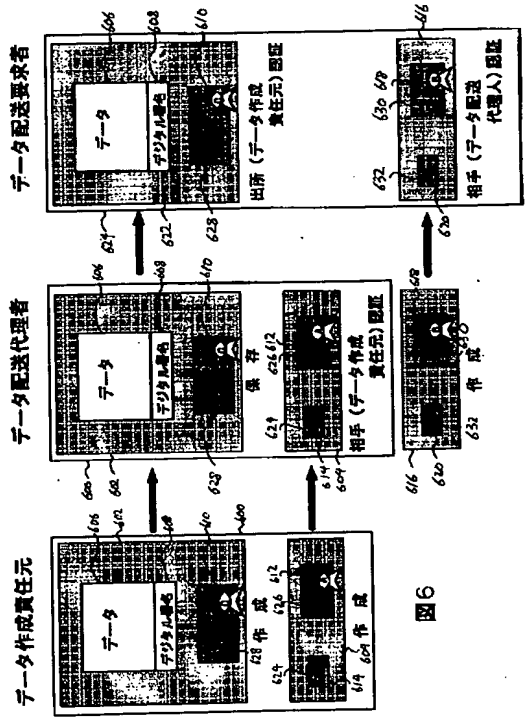


図6

1

【特許請求の範囲】

【請求項１】データを複数者間を経由してデータの発送元と、発送依頼先で安全な通信で送付する場合に、実際に通信する２者間がお互いを認証する手段と、データ最終受取者が発送開始者を認証する手段を分割することを特徴とする出所認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は共通鍵暗号方式と公開鍵暗号方式を用いた電子商取引に関し、特に配布データの作成元／責任元を明確にすることができる、データの出所認証方法に関する。

【０００２】

【従来の技術】商取引をネットワーク、特にインターネットで行う電子商取引においては、買い手は世界中のインターネット上にある仮想店舗にアクセスし、多種多様な商品を購入することができる。また、購入できる商品は、洋服等の形のある「品物」だけでなく、ネットワークを通じて配送できる、ソフトウエア等の形のない「データ」をも含まれる。

【０００３】しかし、インターネットを用いて電子商取引を行う場合にはソフトウエア等のデータのやり取りの安全性が問題となる。つまり、データの漏洩や、改竄、配送元のなりすまし等の犯罪を比較的容易に行うことができるからである。

【０００４】このような問題に対して、共通鍵暗号方式や、公開鍵暗号方式といった暗号化方式を使って、安全なデータのやり取りを実現することが一般的である。ここで、共通鍵暗号方式とは、暗号化する時に使用する鍵と復号化する時に使用する鍵が同じである暗号方式であり、暗・復号速度が高速なので、大量のデータを暗号化するのに適している。これに対して公開鍵暗号方式とは、他者に見せない鍵(秘密鍵)と、それに対応する、他者に公開する鍵(公開鍵)がペアになっていて、一方の鍵を使用して作られた暗号文は、ペアのもう一方の鍵を使用しなければ復号化できない方式であり、不特定多数の人と通信することに適している。

【０００５】また、証明書発行局という、信頼できる第３者機関が発行した電子的な証明書（以下、証明書）を使用することにより、取引相手の身元を証明し、通信元のなりすましを防止する方法が提案されている。証明書発行局は一つとは限らず、通信先、通信元の双方が、信頼できる同じ証明書発行局からの証明書を持っていれば相手の認証が可能である。

【０００６】以下、証明書発行局の証明書を用いた、データ作成責任元(以下、作成責任元)とデータ配送要求者(以下、配送要求者)間での安全なデータのやり取りを行う場合の手順を説明する。

【０００７】まず、配送要求者は証明書をネットワークを通じて作成責任元に送付する。証明書の中には、認証

2

対象者の公開鍵と、それを認証した証明書発行局のデータなどが暗号化されて入っており、認証は双方の電子的な証明書の中に入っている証明書発行局のデータを突き合わせる事で行う。

【０００８】作成責任元は、配送要求者から送られた証明書を、同じ証明書発行局から発行された、証明書を用いて相手認証する。もし認証できたならば、作成責任元は要求されたデータと、データを元に生成したデジタル署名、デジタル署名を復号化する公開鍵の含まれた電子的な証明書を新たに生成した共通鍵で暗号化する。ここで、デジタル署名は、データの改竄を防止する役割をはたす。

【０００９】次に、生成した共通鍵を相手に送付しないと復号化できないため、電子封筒にに入れた送付する。ここで、電子封筒とは、相手先から送付された証明書内の公開鍵で、共通鍵を暗号化したものをさし、送付データの漏洩を防ぐ役割を果たす。そして、電子封筒と、データ等を暗号化したものといっしょに配送要求者へ送付する。

【００１０】配送要求者は、送られてきた電子封筒を配送要求者の秘密鍵で復号し、共通鍵を取り出し、暗号化されたデータを復号する。復号化できたならば、復号化により取り出された作成責任元の証明書と、デジタル署名を用いて、相手認証と、データが改竄されていないかを確かめる。この一連のプロセスにより、２者間での安全なデータの受渡しを実現することができ、２者間の出所認証も実現される。

【００１１】配送要求者と作成責任元の間にデータ配送代行者(以下、配送代行者)が存在し、データ配送代行者経由でデータのやり取りをする場合には、配送要求者の証明書を配送代行者経由で作成責任元に送付し、送付者が証明書内に入っている公開鍵で電子封筒を作成することにより、配送代行者経由で３者間での安全なデータの受渡しを実現し、配送要求者は、作成責任元を認証する事ができる。つまり、作成責任元の出所認証を実現している。

【００１２】しかし、配送要求者の証明書を配送代行者を通して作成責任元に配送し、暗号化する方式では、通信コストが膨大となる。なぜなら、ソフトウエア等のファイルの大きさは膨大になるので、配送代行者はソフトウエアの要求のたびに、データ配送者との間の通信コストがかかり、 また、オンライン通信の場合、配送要求者はデータ配送代行者との間の通信コストのほかに、データ配送代行者とデータ配送者間の通信コストもかかってしまい、非常に非効率である。

【００１３】このような問題に対して、従来は、前述の２者間の安全な配送方式を用いて、配送代行者経由での配送を３者間の非同期な場合と位置づけ、まず、作成責任元と配送代行者間で安全なデータのやり取りを行ない、データを配送代行者に保管しておき、配送要求者が

配送代行者に発送依頼をし、配送要求者と発送代行者間で安全にデータのやり取りをすることによってこの問題を解決している。

【００１４】

【発明が解決しようとする課題】かかる従来の方法においては、次のような問題がある。

【００１５】すなわち、前述の２者間の安全な配送方式を用いて、配送代行者と作成責任者との間の通信と、配送代行者と配送要求者との間の通信に分割し、データを配送代理人のディスクに蓄積させる方法では、配送代理人にデータを改竄される可能性がある。なぜなら、証明書を検証し、デジタル署名にかけられている暗号をはずすことにより配送代理人は、データ作成責任者を認証するので、データ配送代行者の認証のために作り直すことになってしまう。つまり、配送要求者に届くデータに付いている証明書やデジタル署名は配送代行者のものなので、オリジナルの作成者の人称を行なうことが出来なくなる。

【００１６】本発明の目的は、通信コストを下げるためにデータ配送代行者にデータを保管した場合に、送付データの作成責任元を明確化することができる出所認証方法を提供することにある。

【００１７】

【課題を解決するための手段】本発明は、配送代行者を経由したデータ配送の場合の出所認証において、出所認証を行う部分と、二者間通信の相手認証を行う部分を分ける。例えば、デジタル署名と、それを復号化する公開鍵を含んだ証明書で出所認証を行ない、電子封筒内の暗号化された共通鍵とそれを復号化する公開鍵を含んだ証明書をもちいて、二者間通信での相手認証を行う。実際に通信する２者間は、電子封筒部分で、通信先は、通信元を認証することができる。そこが配送代行者などの中継機関ならば、データ、デジタル署名、それを復号化する公開鍵を含んだ証明書を保管しておく。配送代行者から配送要求者へは、配送要求者が配送代行者を認証できるように、電子封筒を新たに作って配送する。このために、配送要求者は、電子封筒部分で配送代行者を認証し、デジタル署名と、それを復号化する公開鍵を含んだ証明書によって、作成責任者を認証、つまり出所認証を行うことができる。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態を詳細に説明する。

【００１９】図１は本発明における、配送代理人を介したデータ配送のシステム構成を示す構成図である。本実施例では、データの作成責任元と、そのデータを要求している者の間に、データの配送の代行者が存在する。また、本実施例において、配送代行者は１つとしたが、複数者存在してもかまわない。

【００２０】図１において、１００は実際にデータを作成した、データの出所を保証する、作成責任元のデータ配送サーバである。１０２はメインメモリ、１０４はディスク装置であって、ディスク装置１０４の中には、データ(１６０)、データのデジタル署名(１６２)、データの出所認証に用いられる証明書と配送代理人との認証を行うための証明書(１６４)、証明書に対応した公開鍵・秘密鍵(１６６)等が格納されている。１１２はディスプレイ、１１４は入力装置であり、データの作成などに用いる。１０８は通信装置であり、ネットワーク回線１１０を介して配送代理人の配送クライアント１２０との通信を行う。１０６はこれらすべてを制御する制御装置である。

【００２１】１２０はデータ作成責任元から配送された暗号化データ、電子封筒の復号、相手認証、データ保管等を行なうための、作成責任元の配送サーバ１００に対する、配送代行者のデータ配送クライアントであり、かつ、配送要求者にデータを配送するためのデータ配送サーバでもある。１２２はメインメモリ、１２４は作成責任元の配送サーバから配送されたデータ(１６０)、デジタル署名(１６２)、証明書(１６４)を保管するディスク装置２であり、１２６は相手認証を行うための証明書や配送要求者が配送代行者を認証するための証明書(１６８)、各証明書に対応した秘密鍵・公開鍵(１７０)等が格納されているディスク装置である。入力装置１３４、ディスプレイ１３６は作成責任元サーバ１００に対する指示操作と相手認証確認に用いられる。１３０は通信装置であり、作成責任元との通信に用いるネットワーク回線１１０、または、配送要求者との通信に用いるネットワーク回線１３２を通じて通信する。１２８はこれらすべてを制御する制御装置である。

【００２２】１４０は配送代理人から受け取り、データの出所認証等を行うためのクライアントである。１４２はメインメモリであり、１４４は、出所認証を行うための証明書や配送代理人の認証をするための証明書(１７２)、証明書に対応した秘密鍵・公開鍵(１７４)等を格納しているディスク装置１である。入力装置１４６、ディスプレイ１４８は配送代理サーバに対する指示操作と出所認証確認に用いられる。１５０はサーバとの通信を行う通信装置であり、１５２はこれらクライアントの制御を行う制御装置である。

【００２３】ここに示した構成は一例であって、もちろんほかの構成もありうる。例えば、データ配送代理人のディスク構成は一つに統合してもかまわない。

【００２４】図２は作成責任元でのデータ暗号化プロセスブロック図である。図３はデータ配送代理人での作成責任元との間のデータ復号、相手認証、データ格納プロセスブロック図である。図４はデータ配送代理人の配送要求元データを出す時のデータ暗号化プロセスブロック図である。図５はデータ配送要求者の配送代行者との間のデータ復号、配送元認証、データ出所認証プロセスブ

ロック図である。また、図６は、配送代理人を介したデータ配送における出所認証プロセスの概要図である。

【００２５】本実施例においては、証明書発行局は、Ａ(作成責任元と配送代理者を認証)、Ｂ(配送代理者と配送要求者を認証)、Ｃ(作成責任者と配送要求者を認証)の３つが存在し、証明書を発行していると仮定する。また、証明書内には各々の証明書発行局に認証された公開鍵が含まれていて、各々の認証局に認証された公開鍵はそれぞれ違う公開鍵だと仮定する。つまり、３者は各々２種類の証明書と、２種類の公開鍵・秘密鍵のペアをもっている。以下では、例えば証明書発行局Ａが発行した作成責任元の証明書は、「作成責任元の証明書Ａ」と表記し、その証明書に含まれる公開鍵、ならびにそれに対応する秘密鍵は、「作成責任元の公開鍵Ａ／秘密鍵Ａ」と表記する。また、本実施例において、共通鍵については、作成責任元で生成するものと配送代理者が生成するものの２種類が使用される。

【００２６】図６において、６００は作成責任元からデータ配送代理者への配送メッセージである。メッセージ６００は、暗号化データ６０２と電子封筒６０４から構成されている。暗号化データ６０２は、配送対象データ６０６、配送データのデジタル署名６０８、作成責任元の公開鍵Ｃ(６２８)を含んだ作成責任元の証明書Ｃ(６１０)が共通鍵６２４で暗号化されている。ここで、本実施例において、共通鍵暗号方式は特願昭63-103919を用いる。

【００２７】電子封筒６０４は、作成責任元の公開鍵Ａ(６２６)を含んだ作成責任元の証明書Ａ(６１２)と、作成責任元の公開鍵(６２６)で暗号化されている暗号化共通鍵６１４が、配送代理者の公開鍵で暗号化されている。ここで、本実施例において、公開鍵暗号方式には特公昭59-50068を用いる。

【００２８】６１６は、配送代理者が作成する電子封筒である。電子封筒６１６は、配送代理者の公開鍵Ｂ(６３０)を含んだ配送代理者の証明書Ｂ(６１８)と、その証明書内の公開鍵(６３２)で暗号化されている暗号化共通鍵６２０が、配送要求者の公開鍵で暗号化されている。

【００２９】６２４は、配送代理者から配送要求者への転送メッセージである。メッセージ６００は、暗号化データ６２２と電子封筒６１６から構成されている。暗号化データ６２２は、データ６０６、デジタル署名６０８、作成責任元の証明書Ｃ(６１０)を、データ配送代理者が新たに生成した、６２０内の共通鍵６２６で暗号化されている。

【００３０】次に、図２、３、４、５のブロック図、図６の出所認証プロセス概要図に基いた、配送代理人を介したデータ配送時の出所認証法について説明する。

【００３１】まず最初に図６を用いて、配送代理人を介したデータ配送における出所認証プロセスの概要を説明する。

【００３２】データ作成責任元は、データ配送要求者が作成責任元を認証できるように暗号化データ６０２を、また、配送代理者が作成責任元を認証できるように電子封筒６０４を作成し、配送代理者に配送する。つまり、電子封筒６０４で作成責任元と配送代行者の間の相手認証を、暗号化データ６０２で出所認証を行なうことになる。データ配送代理人は、電子封筒６０４部分で、作成責任元を認証する。認証できたならば、暗号化データ６０２を６１４内の共通鍵６２４で復号して、データ６０６、デジタル署名６０８、証明書６１０を保管する。配送代行者から配送要求者へは、配送要求者が配送代行者を認証できるように、新たに作成した共通鍵６３２を使って暗号化データ６２２を生成し、また、電子封筒６１６を新たに作って配送する。配送要求者は、電子封筒部分６１６で配送代行者を認証し、暗号化データ６２２部分で、作成責任元を認証、つまり出所認証を行う。

【００３３】次に図２を用いて、作成責任元での配送メッセージ作成プロセスを説明する。

【００３４】はじめに配送代理者が作成責任元に対して、データ配送要求のために、配送代理者の証明書Ａを配送する。次に、配送データのデジタル署名を作成する。本実施例においては、データをハッシュ関数と呼ばれる特殊な関数により、一定の長さのハッシュ値と呼ばれる値に変換したものを、秘密鍵で暗号化する方式を採用する。ハッシュ値は、一意に定まるので配送元で配送するデジタル署名のハッシュ値と、配送先で配送データをハッシュ化したものを突き合わせる事により、改竄を防止する。

【００３５】はじめに、配送対象データをハッシュ関数を用いてハッシュ化し（２００）、作成責任元の秘密鍵Ｃで暗号化し（２０２）、デジタル署名(６０８)を作る。この一連のデジタル署名作成プロセスは２０４に対応する。次に暗号化データを生成するための共通鍵(６２４)を作成（２０６）する。この共通鍵(６２４)を使って、データ(６０６)、デジタル署名(６０８)、作成責任元の証明書Ｃ(６１０)を暗号化する（２０８）。ここまでのプロセス２１０が、図７の暗号化データ６０２の生成に対応する。次に、図６の６０４に対応する電子封筒(６０４)を作成する。まず、２０６で生成した共通鍵(６２４)を作成責任元の秘密鍵Ａで暗号化（２１２）し、その成果物(６１４)と、作成責任元の証明書Ａ(６１２)を、２１８により取り出した、配送代理人の公開鍵Ａで暗号化（２１４）する。この一連の電子封筒生成プロセス（２１６）により、図６の６０４部分が生成される。最後に、２１０、２１４により生成したメッセージ６００をデータ配送代理人に配送する。

【００３６】上述の実施例において、作成責任元での配送メッセージ作成プロセスを、配送代理者の証明書が配送された時点から開始する形態を取っているが、これ

は、作成責任元から配送代行者へ配送をする許可を要求し、それを受けて配送代理者が証明書を配送するような形態にしてもよい。

【００３７】続いて図３を用いて、データ配送代理人での配送認証処理ならびに配送データ等の格納プロセスを説明する。

【００３８】まず、データ作成責任元から受け取った、暗号化データ(６０２)と電子封筒(６０４)のうち、電子封筒(６０４)を、配送代理者の秘密鍵Ａで復号し、暗号化共通鍵(６１４)と、作成責任元の証明書Ａ(６１２)を取り出す（３００）。次に、取り出した証明書(６１２)と同じ証明書発行局で発行された、データ配送代理人の証明書Ａを用いて、配送された証明書が本物かどうかを検証する（３０２）。検証されたら、作成責任元の証明書Ａ(６１２)に含まれている公開鍵Ａ(６２６)を取り出し（３０４）、３０６で、共通鍵(６２４)を取り出す。この、３０２、３０４、３０６のプロセス３０８により、配送代理人はデータ作成責任元を認証することができる。最後に、共通鍵(６２４)を用いて暗号化データ(６０２)を復号化し、データ(６０６)、デジタル署名(６０８)、作成責任元の証明書Ｃ(６１０)を取り出し（３１０）、それらをディスク装置２(１２４)に格納する（３１２）。

【００３９】上述の実施例において、作成責任元が生成した共通鍵(６２４)で暗号化データ６０２を復号化して、データ６０６、デジタル署名６０８、作成責任元の証明書Ｃ(６１０)をディスク２(１２４)に格納する形態をとっているが、復号化せず、暗号化データ６０２と共通鍵６２４をディスク装置２(１２４)に格納する形態を取ってもよい。

【００４０】続いて、図４を用いて、データ配送要求者が、データ配送代理人を認証できるような電子封筒の作成ならびに、暗号化データと新たに作成された電子封筒のデータ配送要求者への配送プロセスを説明する。

【００４１】はじめに配送代理者が作成責任元に対して、データ配送要求のために、配送要求者の証明書Ｂを配送する。証明書を受け取った配送代理者は、ディスク装置２(１２４)からデータ(６０６)、デジタル署名(６０８)、作成責任元の証明書Ｃ(６１０)を取り出し（４００）、プロセス４０２で生成した共通鍵(６３２)を使って暗号化し（４０４）、このプロセス４０６によって、暗号化データ６２２を生成する。次に、データ配送要求者が配送代理人を認証できるような電子封筒６１６を作成する。まず、４０２で生成した共通鍵６３２を、データ配送代理者の秘密鍵Ｂ(６３０)で暗号化（４０８）し、その成果物と、配送代理者の証明書Ｂ(６１８)をデータ配送要求者の公開鍵Ｂで暗号化（４１０）する。この一連の電子封筒生成プロセス（４１２）により、図６の６０４部分が生成される。最後に、４０６、４１２部分をデータ配送要求者に配送する。

【００４２】最後に、図５を用いて、図６の６２４にあたる、データ配送要求者の復号化、相手認証、ならびにデータ出所認証プロセスを説明する。

【００４３】まず、データ配送代理人から受け取った、暗号化データ６２２と電子封筒６１６のうち、電子封筒６１６を、データ配送要求者の秘密鍵Ｂで復号し、暗号化共通鍵(６２０)と、配送代理者の証明書Ｂ(６１８)を取り出す（５００）。次に、データ配送要求者の証明書Ｂを用いて、配送された証明書(６１８)が本物かどうかを検証する（５０２）。検証できたら、証明書内の公開鍵Ｂ(６３０)を取り出し（５０４）、５０６で、暗号化された共通鍵６３２を復号する。この、５０２、５０４、５０６のプロセス５０８により、配送要求者は配送代理人を認証することができる。次に、取り出した共通鍵６３２を用いて暗号化データ６２２を復号し、データ６０６、デジタル署名６０８、作成責任元の証明書Ｃ(６１０)を取り出す（５１０）。データの出所認証をするために、まず、取り出した作成責任者の証明書Ｃ(６１０)を、同じ証明書発行局で発行された、データ配送要求者の証明書Ｃを用いて、配送された証明書が本物かどうかを検証する（５１２）。本物だと確認できたら、証明書(６１０)から作成責任元の公開鍵Ｃ(６２８)を取り出し（５１４）、その鍵(６２８)でデジタル署名(６０８)を復号し、ハッシュ値を取り出す（５１６）。ここまでのプロセス５１２、５１４、５１６により、データ出所認証がなされたことになる。最後に、新たに、データのハッシュ値を計算し（５１８）、５１６で取り出されたハッシュ値と突き合わせることで、改竄されていないかを確かめられる。

【００４４】上述の実施の形態において、３つの証明書発行局を利用した場合を例にとったが、１つの証明書発行局が３者を認証する様な形を取ってもいい。また、公開鍵と秘密鍵のペアは各者１つずつでよく、この公開鍵を各証明書発行局に認証してもらい、証明書を発行してもらう形式でもよい。

【００４５】

【発明の効果】以上に述べたように、本発明によれば、通信コスト低減のためにデータの作成責任者とデータ配送要求者の間にデータ配送代理者を設置し、データを格納させておいても、データ配送要求者はデータの出所認証を安全に行うことができる。

【図面の簡単な説明】

【図１】本発明に関わる、配送代理人を介したデータ配送のシステムブロック図である。

【図２】本発明に関わる、作成責任元でのデータ暗号化プロセスブロック図である。

【図３】本発明に関わる、データ配送代理者でのデータ復号、相手認証、データ格納プロセスブロック図である。

【図４】本発明に関わる、データ配送代理者のデータ暗

9　　10

号化プロセスブロック図である。

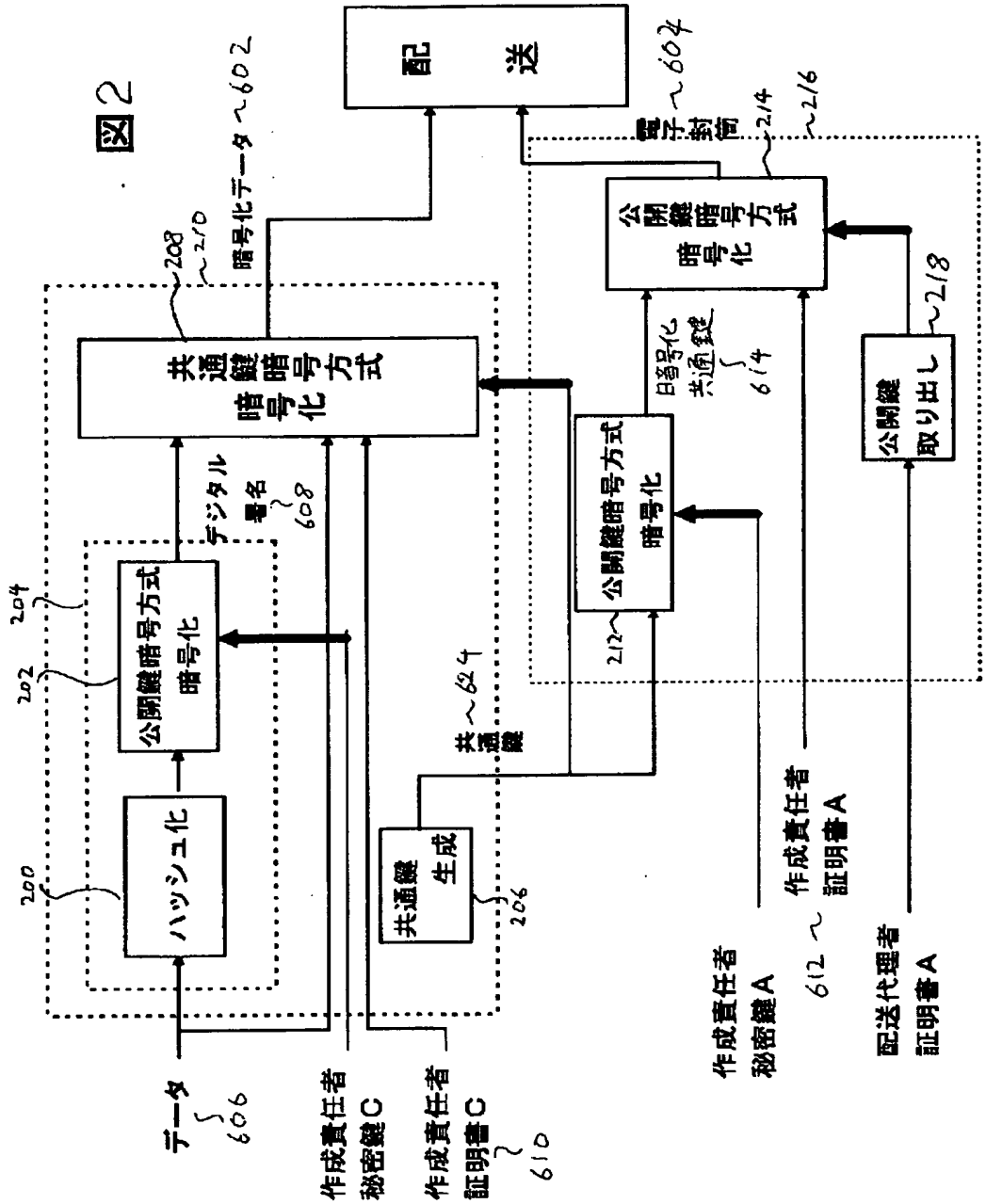
【図５】本発明に関わる、データ配送要求者のデータ復号、配送元認証、データ出所認証プロセスブロック図である。

【図６】本発明に関わる、配送代理人を介したデータ配送における出所認証プロセスの概要図である。

＊【符号の説明】

１００…データ作成責任者側配送サーバ、１２０…データ配送代理人側配送サーバ／クライアント、１４０…データ配送要求者側配送クライアント、６０２…暗号化データ、６０４…電子封筒。

【図２】



【図１】

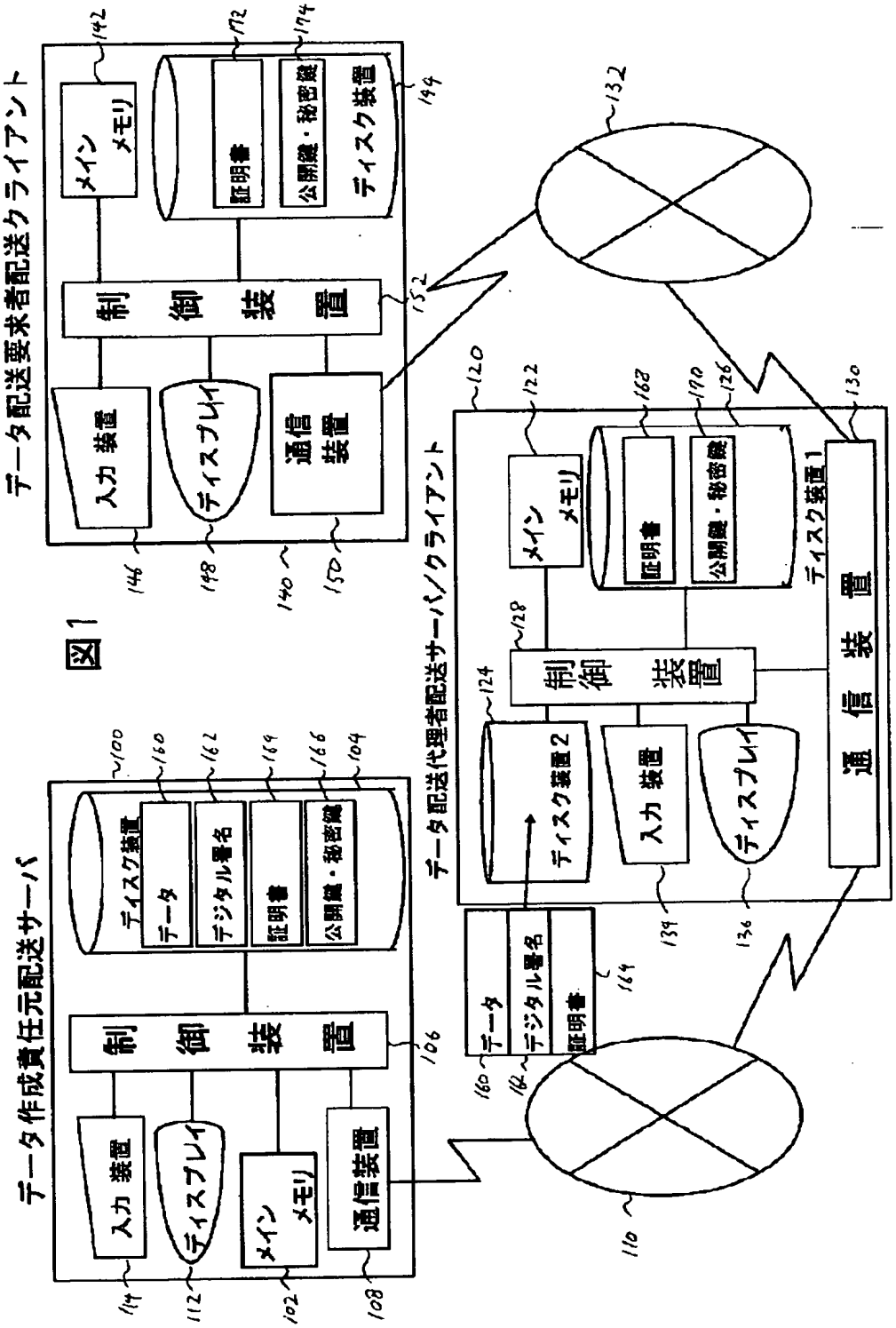

データ配送要求者配送クライアント
メイン メモリ
制 御 装 置
入力 装置
ディスプレイ
通信 装置
証明書
公開鍵・秘密鍵
ディスク装置
データ配送代理者配送サーバ/クライアント
ディスク装置2
ディスク装置1
データ作成責任元配送サーバ
データ
デジタル署名
132
110
142
172
174
149
152
144
148
140
150
120
122
182
190
126
130
128
124
139
136
100
160
162
169
166
104
106
114
112
102
108

図１

【図３】

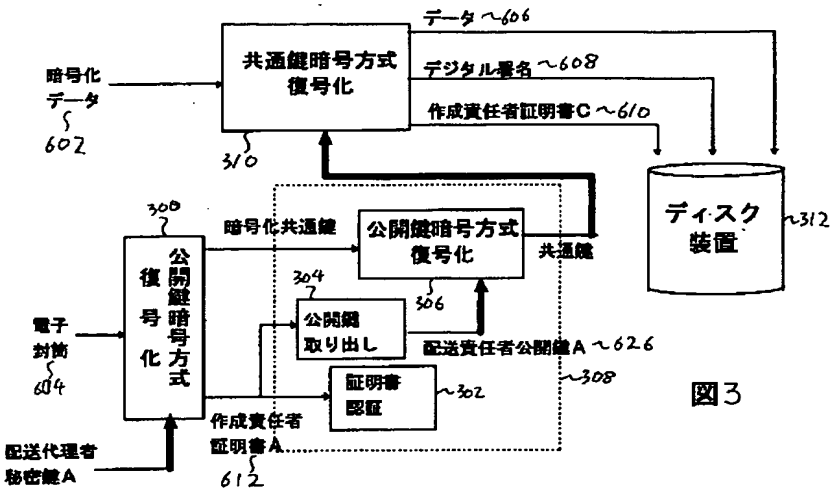

データ
606
共通鍵暗号方式
復号化
デジタル署名
608
作成責任者証明書C
610
暗号化
データ
602
310
300
公開鍵暗号方式
復号化
暗号化共通鍵
共通鍵
ディスク
装置
312
304
公開鍵
取り出し
306
配送責任者公開鍵A
626
308
電子
封筒
604
証明書
認証
302
作成責任者
証明書A
612
配送代理者
秘密鍵A

図３

【図６】

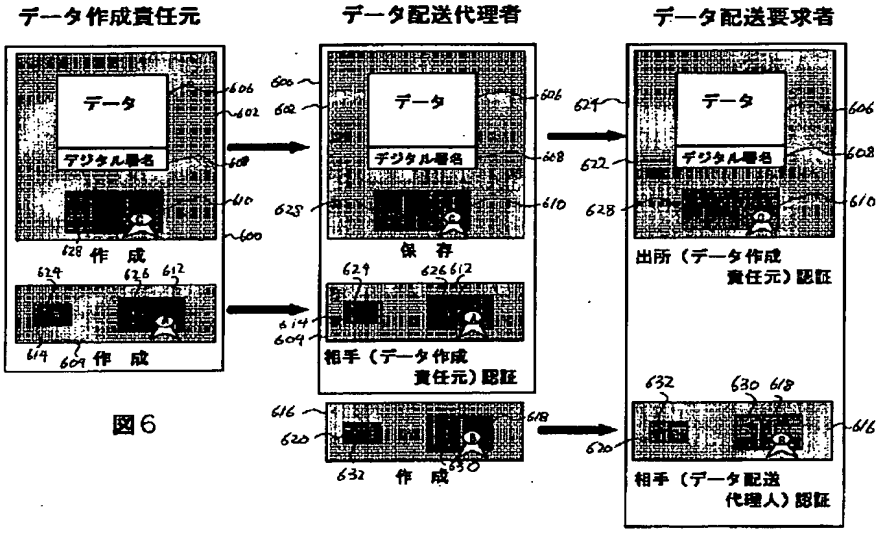

データ作成責任元
データ配送代理者
データ配送要求者
データ
デジタル署名
作成
保存
相手（データ作成
責任元）認証
出所（データ作成
責任元）認証
相手（データ配送
代理人）認証

図６

【図４】

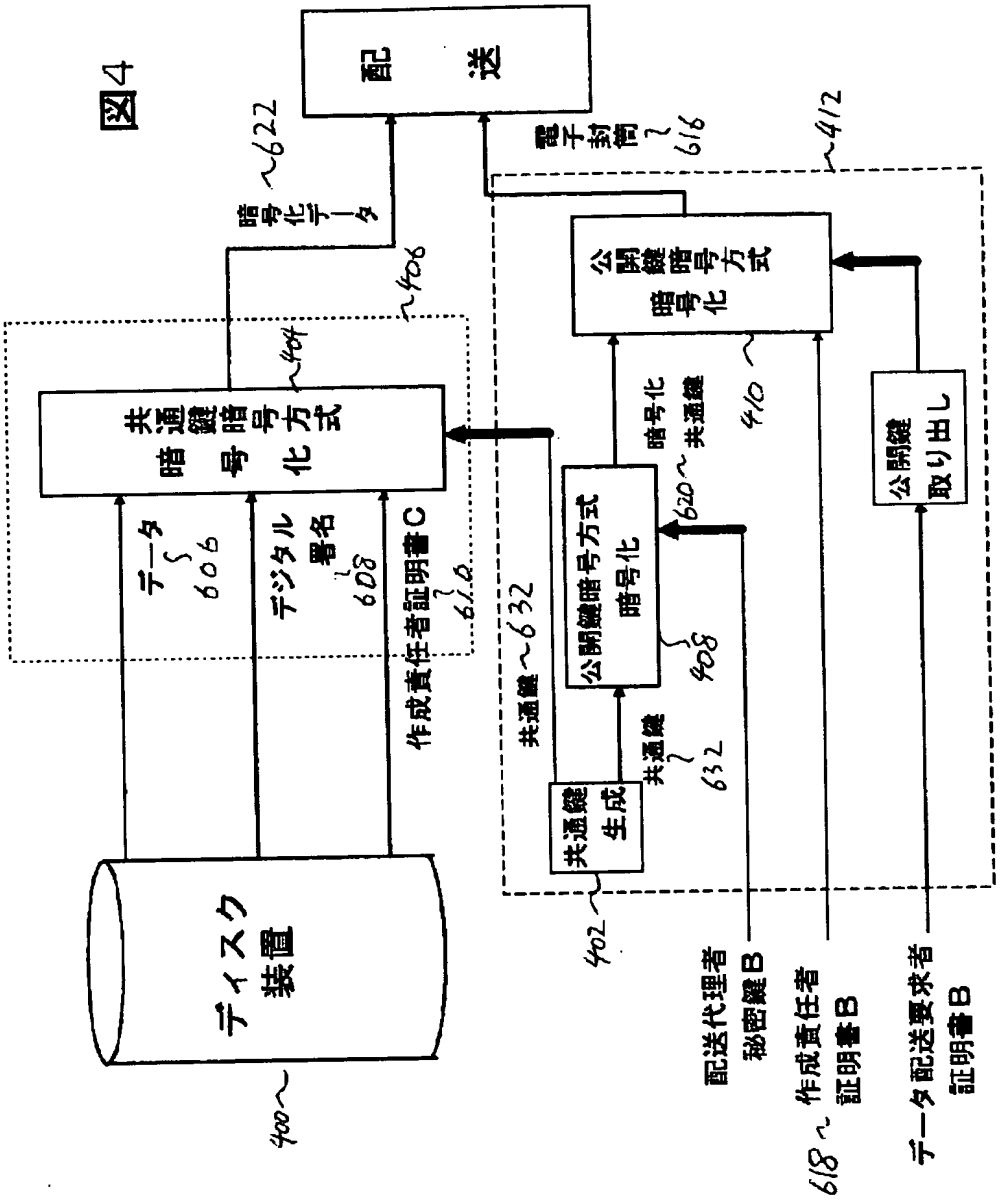


図4
配送
622
暗号化データ
406
404
共通鍵暗号方式
データ
606
デジタル署名
608
作成責任者証明書C
610
400
ディスク装置
412
電子封筒
616
公開鍵暗号方式
410
公開鍵取り出し
620
暗号化共通鍵
公開鍵暗号方式暗号化
408
632
共通鍵
共通鍵生成
402
共通鍵
配送代理者秘密鍵B
618
作成責任者証明書B
データ配送要求者証明書B

【図５】

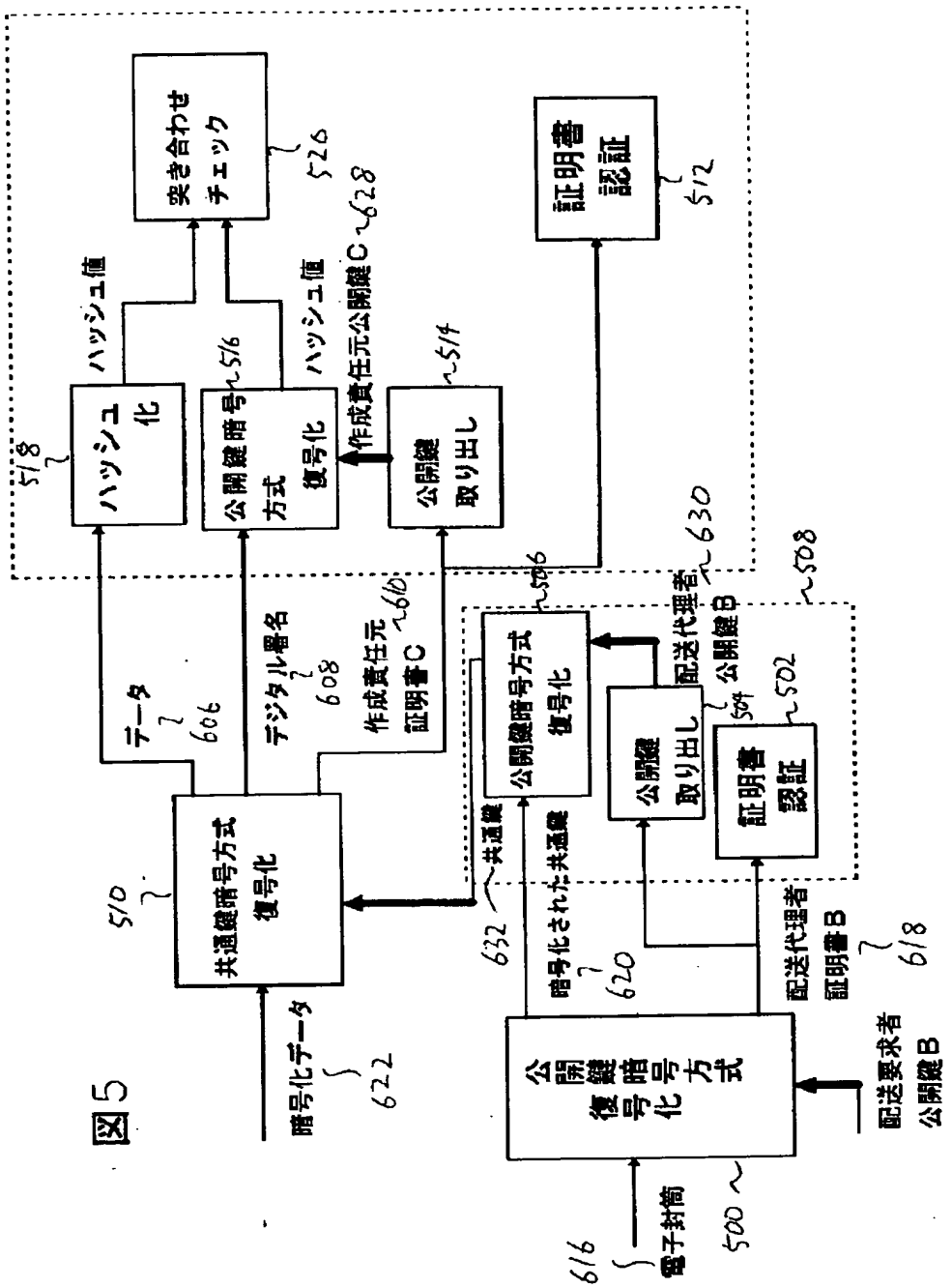


図５

フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
H04L 9/32			G06F 15/21	330	
			H04L 9/00	675A	
				675B	